IN THE CLAIMS

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims in accordance with the following:

1-5. (CANCELLED)

6. (PREVIOUSLY PRESENTED) The system according to claim 10, wherein the open and non-secure wireless network is a wireless local area network.

7. (CANCELLED)

8. (currently amended) The system as in 10 wherein:

the merchant device prompts for input of or stores the second merchant device parameter as the merchant identifying information, and

the ~~trusted secure transaction server~~STS stores the merchant identifying information.

9. (PREVIOUSLY PRESENTED) The system as in claim 10, further comprising one or more payment ~~services executing~~servers comprising a computer processor that provide a payment service upon direction of the ~~trusted secure transaction server~~STS, and

wherein the ~~trusted secure transaction server~~STS is in secure communication with the one or more payment ~~services,~~servers including online payment services, financial institutions, and credit card agencies, using a wired or wireless network and the ~~trusted secure transaction server~~STS directs that payment be ~~executed~~ made by the payment services upon verification of the purchase transaction by the ~~trusted secure transaction server~~STS.

10. (currently amended) A computer system for conducting an agreement between two parties relying on a Secure Transaction Server (STS) as a trusted third party comprising:

a first party consumer mobile device for a consumer and comprising a computer

processor that by execution of instructions~~executes~~:

generates, independent of the second and third parties, ~~generating~~ a first mobile device parameter derived from a stored mobile device parameter and generating a first view of the agreement pertaining to ordering and/or purchasing goods and/or services,

~~securing~~secures the first view of the agreement based upon a key derived from both the generated first mobile device parameter and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile device, and

~~transmitting~~transmits the first view of the agreement to the second party, the first view of the agreement not including the first and second mobile device parameters; and

a second party merchant device for a merchant and comprising a computer processor that by execution of instructions~~executes~~:

~~generating~~generates, independently of the first and third party, a second view of the agreement secured based upon both a first merchant device parameter and a second merchant device parameter as merchant identifying information, and

~~transmitting~~transmits the second secured view of the agreement to the third party,

wherein the first party consumer mobile device and the second party merchant device are ~~in communication~~communicably connectable over an open and non-secure wireless network for connecting the first party and the second party and to transmit ~~transmitting~~ the first view of the agreement from the first party to the second party,

wherein the second party merchant device is ~~in communication~~communicably connectable with the trusted third party server over a wired or wireless network for connecting the second party to the third party and to transmit ~~transmitting~~ the first and second views of the agreement to the trusted third party server,

wherein the ~~trusted third party server~~STS comprises a computer processor that by execution of instructons: ~~executes operations of verifying~~

verifies conditions of the agreement including identities of the first and second parties in the independent secured first and second views of the agreement, based upon a symmetric agreement verification protocol deriving the key based upon the first and second mobile device parameters for the secured first view and using the first and second merchant device parameters for the secured second view, and ~~taking~~takes action to execute ~~executing~~ the agreement according to the verification of the conditions of the agreement, and

~~wherein the STS~~exclusively stores the personal identifying information of the first

party as the second input mobile device parameter.

11. (currently amended) The system as in claim 9, wherein the ~~trusted secure transaction server~~STS supplies a token as confirmation of the payment.

12. (PREVIOUSLY PRESENTED) The system as in claim 11, wherein the merchant device processes the token presented by the consumer to consume the good and/or service.

13. (currently amended) The system as in claim 10, wherein only the ~~trusted secure transaction server~~STS, and neither the merchant device nor the consumer mobile device are able to observe details of other's transaction including the identifying information of the consumer and the merchant.

14. (PREVIOUSLY PRESENTED) The system as in claim 10, wherein the consumer identifying information comprises one or more of a personal identification number (PIN), password, biometric information, a fingerprint or a voiceprint.

15. (currently amended) The system as in claim 14, wherein the consumer mobile device prompts the consumer for authorizing payment through an explicit command to the consumer mobile device by requesting input of the consumer identifying information.

16. (currently amended) The system as in claim 9, wherein the ~~trusted secure transaction server~~STS registers financial account information of the consumer for the payment services, and the consumer mobile device presents selectable financial account information of the consumer from the consumer financial account information registered by the ~~secure transaction server~~STS.

17. (currently amended) The system as in claim 9, wherein the ~~secure transaction server~~STS registers the consumer and the merchant by registering financial account information of the consumer and the merchant, providing the consumer and merchant identifying information, and providing to the consumer mobile device and the merchant device software executing the symmetric agreement verification protocol.

18. (currently amended) The system as in claim 17 wherein:

the consumer mobile device discovers the merchant device;

the consumer mobile device receives consumer selectable goods and/or services for conducting the purchase from the merchant device;

the consumer mobile device obtains from the merchant device, a purchase order;

the consumer mobile device receives payment authorization from the consumer for the purchase order, as the first view of the agreement;

the merchant device receives authorization for acceptance of the consumer payment from the merchant, as the second view of the agreement;

the ~~secure transaction server~~STS verifies the conditions of the agreement;

the ~~secure transaction server~~STS as the action executing the agreement causes payment from the consumer to the merchant through one of the payment services; and

the ~~secure transaction server~~STS issues receipts to the consumer device and to the merchant device indicating success or failure of the transaction.

19. (currently amended) The system of claim 18, wherein the ~~secure transaction server~~STS collects a fee for processing the purchase from one or more of the consumer, merchant, or payment services based on a fee for each purchase or on a percentage of purchase amount.

20. (currently amended) The system as in claim 18, wherein the wired or wireless network connecting the merchant device with the ~~secure transaction server~~STS is a secure network and wherein the open and non-secure wireless network is a wireless local area network operated by the merchant device.

21. (PREVIOUSLY PRESENTED) The system as in claim 20 wherein the wireless local area network includes a hotspot accessible by a plurality of merchant devices and consumer mobile devices and the consumer mobile device provides selectable merchants based upon the merchant devices through the wireless local area network.

22. (CANCELLED)

23. (currently amended) The system as in claim 20, wherein the wireless local area

network includes a hotspot accessible by a plurality of merchant devices and consumer mobile devices, and the consumer mobile device provides selectable merchants based upon the merchant devices through the wireless local area network, and the merchant devices, the consumer devices, and the ~~secure transaction server~~STS are in communication with each other via the hotspot.

24. (PREVIOUSLY PRESENTED) The system as in claim 20, wherein the merchant device executing a retail application and a secure transaction purchasing application, can execute the secure transaction application on a local device at the merchant location connected to the wireless local area network and a remote device connected via another network to the wireless local area network and the consumer device.

25. (currently amended) The system as in any one of claims 19, 20, 21, 23, and 24, wherein the merchant device is connected to the ~~secure transaction server~~STS via Internet using security including a secure socket layer (SSL) or a Virtual Private Network.

26. (currently amended) The system as in any one of claims 19, 20, 21, 23, and 24, wherein the ~~secure transaction server~~STS is connected to one or more of the payment ~~services~~servers through a secure network or through Internet using security including secure socket layer (SSL) or a Virtual Private Network.

27. (currently amended) The system as in claim 18 wherein the consumer mobile devices requests the ~~Secure Transaction Server~~STS to disable the consumer mobile device for a purchase using a current consumer identifying information.

28. (currently amended) The system as in claim 18 where the ~~Secure Transaction Server~~STS detects and disables a consumer account if there are multiple attempts to authorize a payment with incorrect consumer identifying information.

29. (PREVIOUSLY PRESENTED) The system as in claim 18,

wherein one of the services for the purchase is a movie ticket, from the merchant device and wherein the receipt is an electronic token as proof of the payment, and

wherein the consumer mobile device provides the token to obtain the service, including

a paperless e-ticket.

30. (currently amended) The system as in claim 18 where the purchase is a return of goods and/or services from the consumer to the merchant and the ~~secure transaction server~~STS causes payment from the merchant to the consumer.

31. (currently amended) The system as in claim 18 in which the ~~Secure Transaction Server~~STS provides ancillary information from the payment services, including advertisements, special interest rate for a particular purchase if a specific credit account is chosen for an attempted purchase, to the consumer mobile device in response messages prior to the consumer payment authorization.